AO 106 (Rev. 5/85) Affidavit for Search Warrant

United States District Court

DISTRICT OF DELAWARE

In the Matter of the Search of

(Name, address or brief description of person or property to be searched)

[redacted], Newark, DE 19702, described more particularly on Attachment A

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 07- 53M-MPT

REDACTED

I William J. Shields being duly sworn depose and say:

I am a(n) U.S. Immigration & Customs Enforcement Special Agent and have reason to believe
Official Title

that ☐ on the person of or ☒ on the premises known as (name, description and/or location)

[redacted], Newark, DE 19702, described more particularly above

in the District of Delaware

there is now concealed a certain person or property, namely (describe the person or property)

described more particularly on Attachment B

which is (give alleged grounds for search and seizure under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence of a crime and contraband

in violation of Title 18 United States Code, Section(s) 2252 and 2252A

The facts to support the issuance of a Search Warrant are as follows:

AFFIDAVIT attached

FILED
MAY 22 2007
U.S. DISTRICT COURT
DISTRICT OF DELAWARE

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

William J. Shields

Signature of Affiant
William J. Shields, Special Agent
U.S. Immigration & Customs Enforcement

Sworn to before me, and subscribed in my presence

3/22/07 at Wilmington, Delaware
Date City and State

Honorable Mary Pat Thynge
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

ATTACHMENT A - DESCRIPTION OF PROPERTY TO BE SEARCHED

[redacted], Newark, Delaware, 19702, is a one story, single-family mobile home dwelling, located on the north side of [redacted]. The structure has white vinyl siding and a black roof. A peaked gable structure extends up from the roof, in the center of the structure, over the front door. The front of the house has five windows, all framed by green shutters. There is a white door in the approximate middle of the front of the structure. A small porch extends out from the structure in the vicinity of the front door. The number [redacted] in black, is affixed to the structure to the left of the front door. There is no garage attached to the structure or on the property.

ATTACHMENT B - ITEMS TO BE SEARCHED FOR AND SEIZED

1. Images of child pornography, as defined in 18 U.S.C. § 2256, including, but not limited to:

a. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums. The digital images of child pornography are to include the following:

ZIP_Files_YOUNG,

[redacted], which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted], which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted].JPG, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted] which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted]G, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted]JPG, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted] entitle "motherdaugh", which is a video recording depicting a prepubescent female engaging in a sexual act with an adult female.

[redacted], which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted] which depicts a prepubescent male engaging in a sexual act with a teen-aged male.

b. books and magazines;

c. photographs, motion pictures, films, videos, and other recordings.

2. Any and all input/output peripheral devices, including but not limited to passwords, data security devices and hardware/software manuals.

3. Information or correspondence pertaining to the receipt, possession or distribution of child pornography that was transmitted or received using a computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages; and

b. books, ledgers, and records.

4. Records evidencing occupancy or ownership of the subject premises described above, including, but not limited to, deeds, leases, utility and telephone bills.

5. Records or other items which evidence ownership or use of computer equipment found in the subject residence, including, but not limited to: banking records; sales receipts; bills for Internet access, including AOL; use of email addresses [redacted] and [redacted] and correspondence with the following email addresses:

[redacted]

AFFIDAVIT

1. I am a Senior Special Agent with the United States Immigration and Customs Enforcement ("ICE"). I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of search warrants. I have been employed as a Special Agent for the ICE (and its predecessor, the United States Customs Service) for twenty-three years, and am currently assigned to the Wilmington, Delaware, Office of Investigations. I was previously assigned to the Philadelphia Office of Investigations for approximately twenty-one years, where my responsibilities included conducting investigations into financial crimes, commercial fraud, child pornography smuggling, asset removal, and narcotics smuggling.

2. Pursuant to 18 U.S.C. § 2251 et seq. , I am authorized to investigate crimes involving the sexual exploitation of children. Sections 2252 and 2252A make it a federal crime for any person to knowingly receive or distribute child pornography that has been mailed or has been shipped or transported in foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer. That section also makes it illegal to knowingly reproduce any visual depiction for distribution in foreign commerce by any means including by computer or through the mails. I have participated in investigations of persons suspected of violating federal child pornography laws, including Title 18 U.S.C. §§ 2251, 2252 and 2252A.

3. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received training from ICE and its predecessors (the United States Customs Service (USCS)), regarding child pornography, the sexual abuse of children, the behavior of preferential child molesters, and how to conduct investigations of child sexual exploitation and obscenity. In the course of my duties, I have had

contact, in the form of interviews and meetings, with preferential child pornographers and those involved in the distribution, sale, processing and/or producing of child pornography.

4. This Affidavit is made in support of an application for a warrant to search the entire premises located at [redacted] Newark, Delaware, 19702 (the "SUBJECT PREMISES"). The SUBJECT PREMISES to be searched is more particularly described as:

> [redacted] Newark, Delaware, 19702, is a one story, single-family mobile home dwelling, located on the north side of [redacted]. The structure has white vinyl siding and a black roof. A peaked gable structure extends up from the roof, in the center of the structure, over the front door. The front of the house has five windows, all framed by green shutters. There is a white door in the approximate middle of the front of the structure. A small porch extends out from the structure in the vicinity of the front door. The number '[redacted] in black, is affixed to the structure to the left of the front door. There is no garage attached to the structure or on the property.

5. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252 and 2252A, which among other things make it a crime to possess and distribute child pornography in interstate commerce by computer.

6. I am familiar with the information contained in this Affidavit based upon the investigation I have personally conducted and based on my conversations with other law enforcement officers involved in this and other investigations.

7. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A are located at the SUBJECT PREMISES and within a computer and related peripherals, and computer media found at the SUBJECT

PREMISES. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part.

8. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2252 and 2252A, are present at the SUBJECT PREMISES.

The Internet and Definitions of Technical Terms

9. Set forth below are some definitions of technical terms, used throughout this Affidavit, and in Attachments A and B hereto, pertaining to the Internet and computers more generally.

a. **Computer system and related peripherals, and computer media**: As used in this affidavit, the terms "computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, CDs, DVDs, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, compact flash cards, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

b. **MD5 Hash Value:** A hash value, also known as a message digest, is a mathematical value generated by applying an algorithm to a computer file. Hash values play a role in security systems where they are used to ensure that transmitted messages have not been tampered with. An MD5 hash value is 16-character hexadecimal value calculated by applying the MD5 algorithm to a computer file. I have consulted with ICE

Special Agent Doug Green who has informed me that among computer forensics professionals, the MD5 hash value is generally considered to be a unique signature or fingerprint for a file.

c. **Fast Track Hash Value**: A MD5 hash value generated using the first 300KB (307200 bytes) of data from a file.

d. **Internet Service Providers (ISPs) and the Storage of ISP Records**: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content

uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," see 18 U.S.C. § 2510(17), and the provider of such a service is an "electronic communications service." An "electronic communications service," as defined by statute, is "any service, which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." 18 U.S.C. § 2711(2).

e. **IP Address:** Every computer or device on the Internet is referenced by unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiate access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers.

Most ISP's employ dynamic IP addressing that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared serially among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISP's, including most cable providers, employ static IP addressing, that is a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

Computers and Child Pornography

10. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology has revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure

storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently individuals distribute child pornography over the internet, allowing them to remain relatively anonymous.

11. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, those who engage in viewing child pornography also maintain a collection of child pornography. The development of computers has also revolutionized the way in which child pornography collectors interact with, and sexually exploit, children. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage/collection. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer

in that this method of production does not leave as large a trail for law enforcement to follow.

b. The Internet allows any computer to connect to another computer. Electronic contact can be made to literally millions of computers around the world.

c. The Internet allows users, while still maintaining anonymity, to easily locate (I) other individuals with similar interests in child pornography; and (ii) web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 120 or more gigabytes are not uncommon. These drives can store tens of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done,

there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

Probable Cause to Search the Subject Premises

12. In December 2004, ICE and the Fresno County Sheriff's Department (FCSD) initiated a joint investigation of a specific Fresno, California, resident (the Fresno resident) subsequent to the receipt of an investigative lead from the National Center for Missing and Exploited Children (NCMEC). According to NCMEC, an individual utilizing the America Online screen name [redacted] had been detected by America Online representatives uploading an image of child pornography to the America Online email server. The image, later verified by an ICE Special Agent to be child pornography, was uploaded on December 26, 2004, by an individual utilizing the AOL screen name [redacted] Subsequent investigation revealed that [redacted] was registered to the Fresno resident at a specific Fresno, California, address. Based on additional investigation conducted by ICE and FCSD, a federal search warrant was obtained for the residence of the Fresno resident.

13. On January 6, 2005, ICE Special Agents and Fresno County Sheriff's Detectives executed a federal search warrant at the residence of the Fresno resident. Located during the search of a bedroom in the residence were numerous printed images depicting prepubescent children engaging in graphic sexual activity.

14. Also located during the search of the residence was a desktop computer. A trained computer forensic examiner conducted an onsite forensic examination of the computer's hard drive. During the search, in excess of 600 saved images of child pornography were located on the hard drive. The images included depictions of prepubescent children, as young as a few months old,

engaged in actual or simulated acts. Also located during the search were four CD-ROMS, two of which revealed a total of 445 images of child pornography and 41 child pornography movie files. The images included prepubescent children being sexually abused by adults and constitute child pornography, as defined in 18 USC § 2256.

15. During the search, the Fresno resident confessed to obtaining child pornography via the Internet, which he accessed via the Internet Service Provider America Online (AOL). He stated he previously utilized the AOL email/screen nam[redacted]o obtain child pornography, but his account was recently terminated by AOL for unknown reasons (per AOL policy, upon learning a subject is utilizing his/her email to traffic in child pornography the account is automatically terminated). He stated that upon being kicked off of AOL he re-subscribed and was issued a new email address,[redacted] which, according to the Fresno resident, he also utilized to access child pornography. He confessed to the Agents and Detectives that he utilized the Internet to enter AOL chat rooms in which the discussion centered on the sexual exploitation of prepubescent children. He stated that while in the chat rooms he would view, and in engage in, sexually explicit conversations with others for his own sexual arousal and gratification. He further admitted that while in the chat rooms he would both receive and distribute images of child pornography to/from other individuals in the chat room via AOL email. He stated that he would enter the chat rooms at least every two days to trade child pornography with other AOL members. He stated that he primarily traded images in a concerted effort to enhance his own child pornography collection, in furtherance of his own sexual arousal and gratification. During the interview he confessed to trading child pornography for at least six months or longer. He informed the Agents and Detectives that he utilized America Online to obtain and distribute child pornography, via AOL email. During the interview he further and specifically stated that one of the individuals he most actively traded child

pornography with utilized the AOL screen name [redacted] later fully identified as a specific resident of Palmyra, Pennsylvania (the Palmyra resident).

16. Based on the aforementioned information, further investigation was conducted related to the online activities of the Palmyra resident by ICE Agents and Detectives. The investigation resulted in the issuance of a federal search warrant in the Middle District of Pennsylvania, obtained and executed by ICE Agents in May 2005 at the residence of the Palmyra resident. During the search a voluminous amount of child pornography was located on the computer hard drive. A subsequent search of the Palmyra resident's stored email contents, previously obtained via a federal search warrant in March 2005, revealed that he, like the Fresno resident, was involved in the receipt and distribution of child pornography via America Online email systems. The Palmyra resident confessed to ICE Agents that he regularly traded images of child pornography utilizing the AOL screen name [redacted].

17. In furtherance of this investigation, and based on forensic evidence obtained from saved emails from the Fresno resident's computer that had been forwarded to him by the Palmyra resident, on or about April 26, 2005, ICE Agents obtained a federal search warrant for the stored email contents of persons associated with the Fresno and Palmyra residents who were suspected of receiving and/or distributing child pornography via America Online email systems. The search warrant (SW 05-101), signed by the Honorable Sandra M. Snyder, United States Magistrate Judge for the Eastern District of California, authorized the search of stored email contents of twenty-seven individuals suspected of trafficking in child pornography via America Online.

18. On or about May 19, 2005, in response to Search Warrant 05-101, ICE agents received stored email contents for the individuals requested. A review of the contents revealed several of the individuals had saved images and/or movie files of child pornography, as defined in 18 USC § 2256,

in their AOL email folders, and several of these individuals were actively engaging in the trafficking of child pornography with other persons via America Online email systems.

19. A specific review of the stored email contents of a subject utilizing the America Online screen name/email address [redacted] subsequently identified as a specific resident of Lake Mary, Florida, (the Lake Mary resident) revealed that he had received and/or distributed images of child pornography to numerous persons not yet fully identified utilizing AOL email systems. A detailed review by ICE Agents of emails sent and received by [redacted] (a.k.a. the Lake Mary resident) revealed that on or about May 6, 2005, [redacted] received an email containing a child pornography movie file from a subject utilizing the email address [redacted] which address investigators have traced to the SUBJECT PREMISES. A review of the email revealed that it depicted the sexual abuse of a prepubescent girl by an adult male and was also distributed by [redacted] at the same time to a subject utilizing the email account [redacted]

20. Further review of the stored email accounts of [redacted] revealed that the account was utilized to send massive amounts of child pornography to numerous other AOL subscribers. A review of the emails and accompanying file attachments by ICE Agents revealed that the files sent depict child pornography, as defined in 18 USC § 2256. The ICE Agents reached this conclusion, based on review of the files and based on training and experience related to previous child pornography investigations. Specifically, the images depict prepubescent children either being sexually abused by adults, engaging in sexually explicit conduct with one another and/or posing nude in a sexually explicit or lewd and lascivious manner. A detailed review of the child pornography emails sent by [redacted] evealed that a subject utilizing the e-mail address

[redacted] received approximately 18 separate e-mails, containing child pornography file attachments between 04/21/2005 and 05/09/2005.

21. On August 5, 2005, a Federal Search Warrant (Number 05-SW-219) was issued by the Honorable Sandra M. Snyder, U.S. Magistrate Judge for the Eastern District of California, authorizing the search of the AOL stored e-mail account of [redacted] (among others). The search warrant was served upon America Online on August 5, 2005, via Federal Express . America Online complied with the warrant and provided ICE Agents with computer compact discs (CDs) containing stored e-mail contents for the account of [redacted] Review of the stored contents of the account of [redacted] revealed multiple images of child pornography stored in the account. Pursuant to the search warrant, America Online provided information that the AOL subscriber of screen name [redacted] was: Edward Roe, address [redacted] Newark, DE 19702.

22. Your affiant has reviewed the stored images of the AOL account of [redacted] and they include the following titled and described files:

ZIP_Files_YOUNG,

[redacted], which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted]JPG, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted]PG, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted].JPG, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted]JPG, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted].JPG, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted], which is a video recording depicting a prepubescent female engaging in a sexual act with an adult female.

[redacted]PG, which depicts a prepubescent female engaging in a sexual act with an adult male.

[redacted]PG, which depicts a prepubescent male engaging in a sexual act with a teen-aged male.

23. The Fresno investigation also identified a specific Barberton, Ohio, resident (the Barberton resident) as having received and distributed numerous images of child pornography via America Online e-mail. On January 11, 2006, ICE agents executed a Federal Search Warrant at the Barberton resident's home. He was advised of his right sand agreed to give a statement to the ICE agents. He stated that he trades child pornography images via his America Online e-mail account approximately once a week. He estimated that he had distributed "a couple hundred" child pornography images within the last year. He specifically remembered trading child pornography images with [redacted]'.

24. After reviewing his buddy list, the Barberton resident advised that he remembered trading child pornography images with [redacted]" and [redacted]. The Barberton resident could not recall the last time he traded child pornography images with this individual. The Barberton resident could not identify any specific images sent to him by "[redacted]" or "[redacted].

25. In response to a summons, America Online records revealed the following subscriber information on the screen names of the Barberton resident's identified from his buddy list:

[redacted]Edward Roe, [redacted]Newark, DE 19702, (302)[redacted]
Member since October 29, 2004, account terminated on July 14, 2005.

[redacted] Edward Roe, [redacted] Newark, DE 19702, (302) [redacted]
Member since July 17, 2005, account active as of March 17, 2006.

26. Further investigation disclosed additional information on Edward Roe:

Full Name: Edward William Roe
Nickname, as per Delaware Criminal History: Billy
Social Security Number: [redacted]
Date of Birth: [redacted]1957
Delaware Driver's License [redacted]
Possible employer: [redacted] Painting
[redacted] Newport, DE 19804
Position: Painter

27. A review of the New Castle County , Delaware, property ownership and deed transfer records, reflect that Edward Roe is the current owner of the property at [redacted] Newark, DE 19702, referred to as Parcel # [redacted]. A review of Delaware Department of Motor Vehicles Registration records reflects several vehicles registered to Edward W. and [redacted] at [redacted] Newark, DE 19702, including:

2002 Chevrolet Trailblazer, VIN [redacted]

1994 Chevrolet Astro Van, VIN [redacted]

28. On December 28, 2006, AOL provided to your affiant subscriber information for the AOL screen names [redacted] and "[redacted]". AOL records reflected that Edward Roe used both referenced screen names, but that all of Roe's AOL accounts have been terminated.

29. During surveillances of the subject location by your affiant and other ICE Agents, two vehicles have consistently been observed at the subject location: a white, late model, 4-door Chevrolet Trailblazer; and an older, blue, Chevrolet Astro Van.

30. On or about March 7, 2007, your affiant began communicating with Det. Chris Shanahan, New Castle County Police Department, regarding his separate investigation of an individual using

the same above-referenced screen name [redacted] Det. Shanahan advises that he has been in communication with and read the police reports of Det. Dennis Pratl, Orland Park Police Department, Orland Park, Illinois. Det. Pratl reported that as part of a child porn investigation he executed a search warrant in Orland Park, Illinois, on December 17, 2006, at the home of an Orland Park resident. The search of a computer seized from that Orland Park residence disclosed, after forensic examination, two emails, dated and received December 7 and 10, 2006, from [redacted] both emails having attachments which are images of child pornography. After Det. Pratl determined by subpoena that the screen name [redacted] was registered to a Delaware resident, Det. Pratl contacted Det. Shanahan in Delaware and forwarded to him the above-referenced two emails and child pornography attachments. Det. Shanahan has advised your affiant that he has viewed both emails and their attachments. Det. Shanahan advises that the attachments both are images of females approximating the age 9 - 12. The image transmitted on December 7, 2006, depicts the young girl in the lascivious exhibition of the genitals and pubic area. Det. Shanahan advises that the image transmitted December 10, 2006, depicts the young girl in a sex act with two adult men.

31. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the distribution and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Collectors of child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica and video tapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone

numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

32. The undersigned affiant submits that there is probable cause to believe that there is a collector of child pornography at the SUBJECT PREMISES.

33. Finally, based upon the conduct of individuals involved in the collection of child pornography set forth above in paragraph 35, namely, that they tend to maintain their collections at private location for long periods of time, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the SUBJECT PREMISES. Even if such images have been deleted, a forensics examination of the subject computer is likely to recover those images.

Specifics Regarding the Seizure and Searching of Computer Systems

34. Based on my own experience and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer experts in a laboratory or other controlled environment:

a. Computer storage devices, such as hard disks, diskettes, tapes, and laser disks can store the equivalent of hundreds of thousands of pages of information. Additionally,

when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

35. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that

a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

Conclusion

36. Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A, which, among other things, make it a federal crime for any person to knowingly possess, transport or distribute child pornography, have been violated, and that the following

property, evidence, fruits and instrumentalities of these offenses are located at the SUBJECT PREMISES. This affiant requests authority to seize the computer as an instrumentality of the crime.

37. Based upon the foregoing, this affiant respectfully requests that this Court issue a search warrant for the SUBJECT PREMISES, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

William J. Shields
Special Agent, ICE

Sworn and Subscribed before me

this 22 day of March, 2007

HONORABLE MARY PAT THYNGE
United States Magistrate Judge